CLAIMS

1. A method of detecting malicious content comprising:

examining at least two characteristics of a digital object;

analyzing said at least two characteristics to determine whether there exists a mismatch therebetween; and

upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

2. A method for detecting malicious content according to claim 1 and wherein said malicious content comprises malicious code.

3. A method for detecting malicious content according to claim 1 and wherein said malicious content comprises masqueraded content.

4. A method for detecting malicious content according to claim 1 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;

file content;

file name extension; and

file icon.

5. A method for detecting malicious content according to claim 4 and wherein said malicious content comprises malicious code.

6. A method for detecting malicious content according to claim 4 and wherein said malicious content comprises masqueraded content.

7. A method for detecting malicious content according to claim 1 and wherein said digital object is selected from a set consisting of:

a file;

an e-mail attachment;

a web page; and

a storage medium.

8. A method for detecting malicious content according to claim 7 and wherein said malicious content comprises malicious code.

9. A method for detecting malicious content according to claim 7 and wherein said malicious content comprises masqueraded content.

10. A method for detecting malicious content according to claim 7 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;

file content;

file name extension; and

file icon.

11. A method for detecting malicious content according to claim 10 and wherein said malicious content comprises malicious code.

12. A method for detecting malicious content according to claim 10 and wherein said malicious content comprises masqueraded content.

13. A method for detecting malicious content according to claim 1 and wherein said digital object comprises a file.

14. A method for detecting malicious content according to claim 1 and wherein said digital object comprises an e-mail attachment.

15. A method for detecting malicious content according to claim 1 and wherein said digital object comprises a web page.

16. A method for detecting malicious content according to claim 1 and wherein said digital object comprises a storage medium.

17. A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

header information; and

file content.

18. A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

header information; and

file name extension.

19. A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

header information; and

file icon.

20. A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

file content; and

file icon.

21. A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

file name extension; and

file icon.

22. A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

file name extension; and

file content.

23. A method of detecting malicious content comprising:

obtaining information relating to at least two characteristics of a digital object;

analyzing said information to categorize said digital object into at least two categories;

comparing said at least two categories to decide whether there exists a mismatch therebetween;

upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

24. A method for detecting malicious content according to claim 23 and wherein said malicious content comprises malicious code.

25. A method for detecting malicious content according to claim 23 and wherein said malicious content comprises masqueraded content.

26. A method for detecting malicious content according to claim 23 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

27. A method for detecting malicious content according to claim 26 and wherein said malicious content comprises malicious code.

28. A method for detecting malicious content according to claim 26 and wherein said malicious content comprises masqueraded content.

29. A method for detecting malicious content according to claim 23 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

30. A method for detecting malicious content according to claim 29 and wherein said malicious content comprises malicious code.

31. A method for detecting malicious content according to claim 29 and wherein said malicious content comprises masqueraded content.

32. A method for detecting malicious content according to claim 29 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

33. A method for detecting malicious content according to claim 32 and wherein said malicious content comprises malicious code.

34. A method for detecting malicious content according to claim 32 and wherein said malicious content comprises masqueraded content.

35. A method for detecting malicious content according to claim 23 and wherein said digital object comprises a file.

36. A method for detecting malicious content according to claim 23 and wherein said digital object comprises an e-mail attachment.

37. A method for detecting malicious content according to claim 23 and wherein said digital object comprises a web page.

38. A method for detecting malicious content according to claim 23 and wherein said digital object comprises a storage medium.

39. A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

header information; and

file content.

40. A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

header information; and

file name extension.

41. A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

header information; and

file icon.

42. A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

file content; and

file icon.

43. A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

file name extension; and

file icon.

44. A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

file name extension; and

file content.

45. A method of detecting malicious content comprising:

examining at least two characteristics of a digital object, each of which characteristics may be selected by a creator of the digital object independently of selection of another characteristic;

analyzing said at least two characteristics to determine whether there exists a mismatch therebetween; and

upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

46. A method for detecting malicious content according to claim 45 and wherein said malicious content comprises malicious code.

47. A method for detecting malicious content according to claim 45 and wherein said malicious content comprises masqueraded content.

48. A method for detecting malicious content according to claim 45 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;

file content;

file name extension; and

file icon.

49. A method for detecting malicious content according to claim 48 and wherein said malicious content comprises malicious code.

50. A method for detecting malicious content according to claim 48 and wherein said malicious content comprises masqueraded content.

51. A method for detecting malicious content according to claim 45 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

52. A method for detecting malicious content according to claim 51 and wherein said malicious content comprises malicious code.

53. A method for detecting malicious content according to claim 51 and wherein said malicious content comprises masqueraded content.

54. A method for detecting malicious content according to claim 51 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

55. A method for detecting malicious content according to claim 54 and wherein said malicious content comprises malicious code.

56. A method for detecting malicious content according to claim 54 and wherein said malicious content comprises masqueraded content.

57. A method for detecting malicious content according to claim 45 and wherein said digital object comprises a file.

58. A method for detecting malicious content according to claim 45 and wherein said digital object comprises an e-mail attachment.

59. A method for detecting malicious content according to claim 45 and wherein said digital object comprises a web page.

60. A method for detecting malicious content according to claim 45 and wherein said digital object comprises a storage medium.

61. A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

header information; and

file content.

62. A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

header information; and

file name extension.

63. A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

header information; and

file icon.

64. A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

file content; and

file icon.

65. A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

file name extension; and

file icon.

66. A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

file name extension; and

file content.

67. A system for detecting malicious content comprising:

a digital object examiner, examining at least two characteristics of a digital object;

a characteristics mismatch detector, analyzing said at least two characteristics to determine whether there exists a mismatch therebetween; and

a digital object classifier, operative upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

68. A system for detecting malicious content according to claim 67 and wherein said malicious content comprises malicious code.

69. A system for detecting malicious content according to claim 67 and wherein said malicious content comprises masqueraded content.

70. A system for detecting malicious content according to claim 67 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;

file content;

file name extension; and

file icon.

71. A system for detecting malicious content according to claim 70 and wherein said malicious content comprises malicious code.

72. A system for detecting malicious content according to claim 70 and wherein said malicious content comprises masqueraded content.

73. A system for detecting malicious content according to claim 67 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

74. A system for detecting malicious content according to claim 73 and wherein said malicious content comprises malicious code.

75. A system for detecting malicious content according to claim 73 and wherein said malicious content comprises masqueraded content.

76. A system for detecting malicious content according to claim 73 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

77. A system for detecting malicious content according to claim 76 and wherein said malicious content comprises malicious code.

78. A system for detecting malicious content according to claim 76 and wherein said malicious content comprises masqueraded content.

79. A system for detecting malicious content according to claim 67 and wherein said digital object comprises a file.

80. A system for detecting malicious content according to claim 67 and wherein said digital object comprises an e-mail attachment.

81. A system for detecting malicious content according to claim 67 and wherein said digital object comprises a web page.

82. A system for detecting malicious content according to claim 67 and wherein said digital object comprises a storage medium.

83. A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

header information; and

file content.

84. A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

header information; and

file name extension.

85. A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

header information; and

file icon.

86. A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

file content; and

file icon.

87. A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

file name extension; and

file icon.

88. A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

file name extension; and

file content.

89. A system according to claim 67 and wherein:

said digital object examiner comprises a digital object examiner server subsystem;

said characteristics mismatch detector comprising a mismatch detector server subsystem; and

said digital object classifier comprising a mismatch detector server subsystem.

90. A system for detecting malicious content according to claim 89 and wherein said malicious content comprises malicious code.

91. A system for detecting malicious content according to claim 89 and wherein said malicious content comprises masqueraded content.

92. A system for detecting malicious content according to claim 89 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;

file content;

file name extension; and

file icon.

93. A system for detecting malicious content according to claim 92 and wherein said malicious content comprises malicious code.

94. A system for detecting malicious content according to claim 92 and wherein said malicious content comprises masqueraded content.

95. A system for detecting malicious content according to claim 89 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

96. A system for detecting malicious content according to claim 95 and wherein said malicious content comprises malicious code.

97. A system for detecting malicious content according to claim 95 and wherein said malicious content comprises masqueraded content.

98. A system for detecting malicious content according to claim 95 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

99. A system for detecting malicious content according to claim 98 and wherein said malicious content comprises malicious code.

100. A system for detecting malicious content according to claim 98 and wherein said malicious content comprises masqueraded content.

101. A system according to claim 67 and wherein:

said digital object examiner comprises a digital object examiner client subsystem;

said characteristics mismatch detector comprising a mismatch detector client subsystem; and

said digital object classifier comprising a mismatch detector client subsystem.

102. A system for detecting malicious content according to claim 101 and wherein said malicious content comprises malicious code.

103. A system for detecting malicious content according to claim 101 and wherein said malicious content comprises masqueraded content.

104. A system for detecting malicious content according to claim 101 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

105. A system for detecting malicious content according to claim 104 and wherein said malicious content comprises malicious code.

106. A system for detecting malicious content according to claim 105 and wherein said malicious content comprises masqueraded content.

107. A system for detecting malicious content according to claim 101 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

108. A system for detecting malicious content according to claim 107 and wherein said malicious content comprises malicious code.

109. A system for detecting malicious content according to claim 107 and wherein said malicious content comprises masqueraded content.

110. A system for detecting malicious content according to claim 107 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

111. A system for detecting malicious content according to claim 110 and wherein said malicious content comprises malicious code.

112. A system for detecting malicious content according to claim 110 and wherein said malicious content comprises masqueraded content.

113. A system according to claim 67 and wherein:

said digital object examiner comprises a digital object examiner gateway subsystem;

said characteristics mismatch detector comprising a mismatch detector gateway subsystem; and said digital object classifier comprising a mismatch detector gateway subsystem.

114. A system for detecting malicious content according to claim 113 and wherein said malicious content comprises malicious code.

115. A system for detecting malicious content according to claim 113 and wherein said malicious content comprises masqueraded content.

116. A system for detecting malicious content according to claim 113 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

117. A system for detecting malicious content according to claim 116 and wherein said malicious content comprises malicious code.

118. A system for detecting malicious content according to claim 116 and wherein said malicious content comprises masqueraded content.

119. A system for detecting malicious content according to claim 113 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

120. A system for detecting malicious content according to claim 119 and wherein said malicious content comprises malicious code.

121. A system for detecting malicious content according to claim 119 and wherein said malicious content comprises masqueraded content.

122. A system for detecting malicious content according to claim 119 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

123. A system for detecting malicious content according to claim 122 and wherein said malicious content comprises malicious code.

124. A system for detecting malicious content according to claim 122 and wherein said malicious content comprises masqueraded content.

125. A system according to claim 67 and wherein:

said digital object examiner is selected from a set consisting of:

a digital object examiner server subsystem;
a digital object examiner client subsystem;
a digital object examiner gateway subsystem;

said digital characteristics mismatch detector is selected from a set consisting of:

a characteristics mismatch detector server subsystem;
a characteristics mismatch detector client subsystem;
a characteristics mismatch detector gateway subsystem;

and

said digital object classifier is selected from a set consisting of:

a digital object classifier server subsystem;
a digital object classifier client subsystem;

a digital object classifier gateway subsystem.

126. A system for detecting malicious content comprising:

a digital object information obtainer, obtaining information related to at least two characteristics of a digital object;

a characteristic based categorizer, categorizing said information into at least two categories;

a categories mismatch detector, analyzing said at least two categories to determine whether there exists a mismatch therebetween; and

a digital object classifier, operative upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

127. A system for detecting malicious content according to claim 126 and wherein said malicious content comprises malicious code.

128. A system for detecting malicious content according to claim 126 and wherein said malicious content comprises masqueraded content.

129. A system for detecting malicious content according to claim 126 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

130. A system for detecting malicious content according to claim 129 and wherein said malicious content comprises malicious code.

131. A system for detecting malicious content according to claim 129 and wherein said malicious content comprises masqueraded content.

132. A system for detecting malicious content according to claim 126 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

133. A system for detecting malicious content according to claim 132 and wherein said malicious content comprises malicious code.

134. A system for detecting malicious content according to claim 132 and wherein said malicious content comprises masqueraded content.

135. A system for detecting malicious content according to claim 132 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

136. A system for detecting malicious content according to claim 135 and wherein said malicious content comprises malicious code.

137. A system for detecting malicious content according to claim 135 and wherein said malicious content comprises masqueraded content.

138. A system for detecting malicious content according to claim 126 and wherein said digital object comprises a file.

139. A system for detecting malicious content according to claim 126 and wherein said digital object comprises an e-mail attachment.

140. A system for detecting malicious content according to claim 126 and wherein said digital object comprises a web page.

141. A system for detecting malicious content according to claim 126 and wherein said digital object comprises a storage medium.

142. A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

header information; and

file content.

143. A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

header information; and

file name extension.

144. A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

header information; and

file icon.

145. A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

file content; and

file icon.

146. A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

file name extension; and

file icon.

147. A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

file name extension; and

file content.

148. A system according to claim 126 and wherein:

said digital object information obtainer comprises a digital object information obtainer server subsystem;

said characteristic based categorizer comprises a characteristic based categorizer server subsystem;

said categories mismatch detector comprising a mismatch detector server subsystem; and

said digital object classifier comprising a mismatch detector server subsystem.

149. A system for detecting malicious content according to claim 148 and wherein said malicious content comprises malicious code.

150. A system for detecting malicious content according to claim 148 and wherein said malicious content comprises masqueraded content.

151. A system for detecting malicious content according to claim 148 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;

file content;

file name extension; and

file icon.

152. A system for detecting malicious content according to claim 151 and wherein said malicious content comprises malicious code.

153. A system for detecting malicious content according to claim 151 and wherein said malicious content comprises masqueraded content.

154. A system for detecting malicious content according to claim 148 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

155. A system for detecting malicious content according to claim 154 and wherein said malicious content comprises malicious code.

156. A system for detecting malicious content according to claim 154 and wherein said malicious content comprises masqueraded content.

157. A system for detecting malicious content according to claim 154 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

158. A system for detecting malicious content according to claim 157 and wherein said malicious content comprises malicious code.

159. A system for detecting malicious content according to claim 157 and wherein said malicious content comprises masqueraded content.

160. A system according to claim 126 and wherein:

said digital object information obtainer comprises a digital object information obtainer client subsystem;

said characteristic based categorizer comprises a characteristic based categorizer client subsystem;

said categories mismatch detector comprising a mismatch detector client subsystem; and

said digital object classifier comprising a mismatch detector client subsystem.

161. A system for detecting malicious content according to claim 160 and wherein said malicious content comprises malicious code.

162. A system for detecting malicious content according to claim 160 and wherein said malicious content comprises masqueraded content.

163. A system for detecting malicious content according to claim 160 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

164. A system for detecting malicious content according to claim 163 and wherein said malicious content comprises malicious code.

165. A system for detecting malicious content according to claim 164 and wherein said malicious content comprises masqueraded content.

166. A system for detecting malicious content according to claim 160 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

167. A system for detecting malicious content according to claim 166 and wherein said malicious content comprises malicious code.

168. A system for detecting malicious content according to claim 166 and wherein said malicious content comprises masqueraded content.

169. A system for detecting malicious content according to claim 166 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

170. A system for detecting malicious content according to claim 169 and wherein said malicious content comprises malicious code.

171. A system for detecting malicious content according to claim 169 and wherein said malicious content comprises masqueraded content.

172. A system according to claim 126 and wherein:

said digital object information obtainer comprises a digital object information obtainer gateway subsystem;

said characteristic based categorizer comprises a characteristic based categorizer gateway subsystem;

said categories mismatch detector comprising a mismatch detector gateway subsystem; and

said digital object classifier comprising a mismatch detector gateway subsystem.

173. A system for detecting malicious content according to claim 172 and wherein said malicious content comprises malicious code.

174. A system for detecting malicious content according to claim 172 and wherein said malicious content comprises masqueraded content.

175. A system for detecting malicious content according to claim 172 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

176. A system for detecting malicious content according to claim 175 and wherein said malicious content comprises malicious code.

177. A system for detecting malicious contént according to claim 175 and wherein said malicious content comprises masqueraded content.

178. A system for detecting malicious content according to claim 172 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

179. A system for detecting malicious content according to claim 178 and wherein said malicious content comprises malicious code.

180. A system for detecting malicious content according to claim 178 and wherein said malicious content comprises masqueraded content.

181. A system for detecting malicious content according to claim 178 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

182. A system for detecting malicious content according to claim 181 and wherein said malicious content comprises malicious code.

183. A system for detecting malicious content according to claim 181 and wherein said malicious content comprises masqueraded content.

184. A system according to claim 126 and wherein:

said digital object information obtainer is selected from a set consisting of:

a digital object information server subsystem;
a digital object information client subsystem;
a digital object information gateway subsystem;

said characteristic based categorizer is selected from a set consisting of:

a characteristic based categorizer server subsystem;
a characteristic based categorizer client subsystem;
a characteristic based categorizer gateway subsystem;

said categories mismatch detector is selected from a set consisting of:

a categories mismatch detector server subsystem;

a categories mismatch detector client subsystem;

a categories mismatch detector gateway subsystem;

and

said digital object classifier is selected from a set consisting of:

a digital object classifier server subsystem;

a digital object classifier client subsystem;

a digital object classifier gateway subsystem.

185. A system for detecting malicious content comprising:

a digital object examiner, examining at least two characteristics of a digital object, each of which characteristics may be selected by a creator of the digital object independently of selection of another characteristic;

a characteristics mismatch detector, analyzing said at least two characteristics to determine whether there exists a mismatch therebetween; and

a digital object classifier, operative upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

186. A system for detecting malicious content according to claim 185 and wherein said malicious content comprises malicious code.

187. A system for detecting malicious content according to claim 185 and wherein said malicious content comprises masqueraded content.

188. A system for detecting malicious content according to claim 185 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;

file content;

file name extension; and

file icon.

189. A system for detecting malicious content according to claim 188 and wherein said malicious content comprises malicious code.

190. A system for detecting malicious content according to claim 188 and wherein said malicious content comprises masqueraded content.

191. A system for detecting malicious content according to claim 185 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

192. A system for detecting malicious content according to claim 191 and wherein said malicious content comprises malicious code.

193. A system for detecting malicious content according to claim 191 and wherein said malicious content comprises masqueraded content.

194. A system for detecting malicious content according to claim 191 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

195. A system for detecting malicious content according to claim 194 and wherein said malicious content comprises malicious code.

196. A system for detecting malicious content according to claim 194 and wherein said malicious content comprises masqueraded content.

197. A system for detecting malicious content according to claim 185 and wherein said digital object comprises a file.

198. A system for detecting malicious content according to claim 185 and wherein said digital object comprises an e-mail attachment.

199. A system for detecting malicious content according to claim 185 and wherein said digital object comprises a web page.

200. A system for detecting malicious content according to claim 185 and wherein said digital object comprises a storage medium.

201. A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

header information; and

file content.

202. A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

header information; and

file name extension.

203. A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

header information; and

file icon.

204. A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

file content; and

file icon.

205. A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

file name extension; and

file icon.

206. A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

file name extension; and

file content.

207. A system according to claim 185 and wherein:

said digital object examiner comprises a digital object examiner server subsystem;

said characteristics mismatch detector comprising a mismatch detector server subsystem; and

said digital object classifier comprising a mismatch detector server subsystem.

208. A system for detecting malicious content according to claim 207 and wherein said malicious content comprises malicious code.

209. A system for detecting malicious content according to claim 207 and wherein said malicious content comprises masqueraded content.

210. A system for detecting malicious content according to claim 207 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;

file content;

file name extension; and

file icon.

211. A system for detecting malicious content according to claim 210 and wherein said malicious content comprises malicious code.

212. A system for detecting malicious content according to claim 210 and wherein said malicious content comprises masqueraded content.

213. A system for detecting malicious content according to claim 207 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

214. A system for detecting malicious content according to claim 213 and wherein said malicious content comprises malicious code.

215. A system for detecting malicious content according to claim 213 and wherein said malicious content comprises masqueraded content.

216. A system for detecting malicious content according to claim 213 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

217. A system for detecting malicious content according to claim 216 and wherein said malicious content comprises malicious code.

218. A system for detecting malicious content according to claim 216 and wherein said malicious content comprises masqueraded content.

219. A system according to claim 185 and wherein:

said digital object examiner comprises a digital object examiner client subsystem;

said characteristics mismatch detector comprising a mismatch detector client subsystem; and

said digital object classifier comprising a mismatch detector client subsystem.

220. A system for detecting malicious content according to claim 219 and wherein said malicious content comprises malicious code.

221. A system for detecting malicious content according to claim 219 and wherein said malicious content comprises masqueraded content.

222. A system for detecting malicious content according to claim 219 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

223. A system for detecting malicious content according to claim 222 and wherein said malicious content comprises malicious code.

224. A system for detecting malicious content according to claim 223 and wherein said malicious content comprises masqueraded content.

225. A system for detecting malicious content according to claim 219 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

226. A system for detecting malicious content according to claim 225 and wherein said malicious content comprises malicious code.

227. A system for detecting malicious content according to claim 225 and wherein said malicious content comprises masqueraded content.

228. A system for detecting malicious content according to claim 225 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

229. A system for detecting malicious content according to claim 228 and wherein said malicious content comprises malicious code.

230. A system for detecting malicious content according to claim 228 and wherein said malicious content comprises masqueraded content.

231. A system according to claim 185 and wherein:

said digital object examiner comprises a digital object examiner gateway subsystem;

said characteristics mismatch detector comprising a mismatch detector gateway subsystem; and said digital object classifier comprising a mismatch detector gateway subsystem.

232. A system for detecting malicious content according to claim 231 and wherein said malicious content comprises malicious code.

233. A system for detecting malicious content according to claim 231 and wherein said malicious content comprises masqueraded content.

234. A system for detecting malicious content according to claim 231 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

235. A system for detecting malicious content according to claim 234 and wherein said malicious content comprises malicious code.

236. A system for detecting malicious content according to claim 234 and wherein said malicious content comprises masqueraded content.

237. A system for detecting malicious content according to claim 231 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

238. A system for detecting malicious content according to claim 237 and wherein said malicious content comprises malicious code.

239. A system for detecting malicious content according to claim 237 and wherein said malicious content comprises masqueraded content.

240. A system for detecting malicious content according to claim 237 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

241. A system for detecting malicious content according to claim 240 and wherein said malicious content comprises malicious code.

242. A system for detecting malicious content according to claim 240 and wherein said malicious content comprises masqueraded content.

243. A system according to claim 185 and wherein:

said digital object examiner is selected from a set consisting of:

a digital object examiner server subsystem;
a digital object examiner client subsystem;
a digital object examiner gateway subsystem;

said digital characteristics mismatch detector is selected from a set consisting of:

a characteristics mismatch detector server subsystem;
a characteristics mismatch detector client subsystem;
a characteristics mismatch detector gateway subsystem;

and

said digital object classifier is selected from a set consisting of:

a digital object classifier server subsystem;
a digital object classifier client subsystem;

a digital object classifier gateway subsystem.